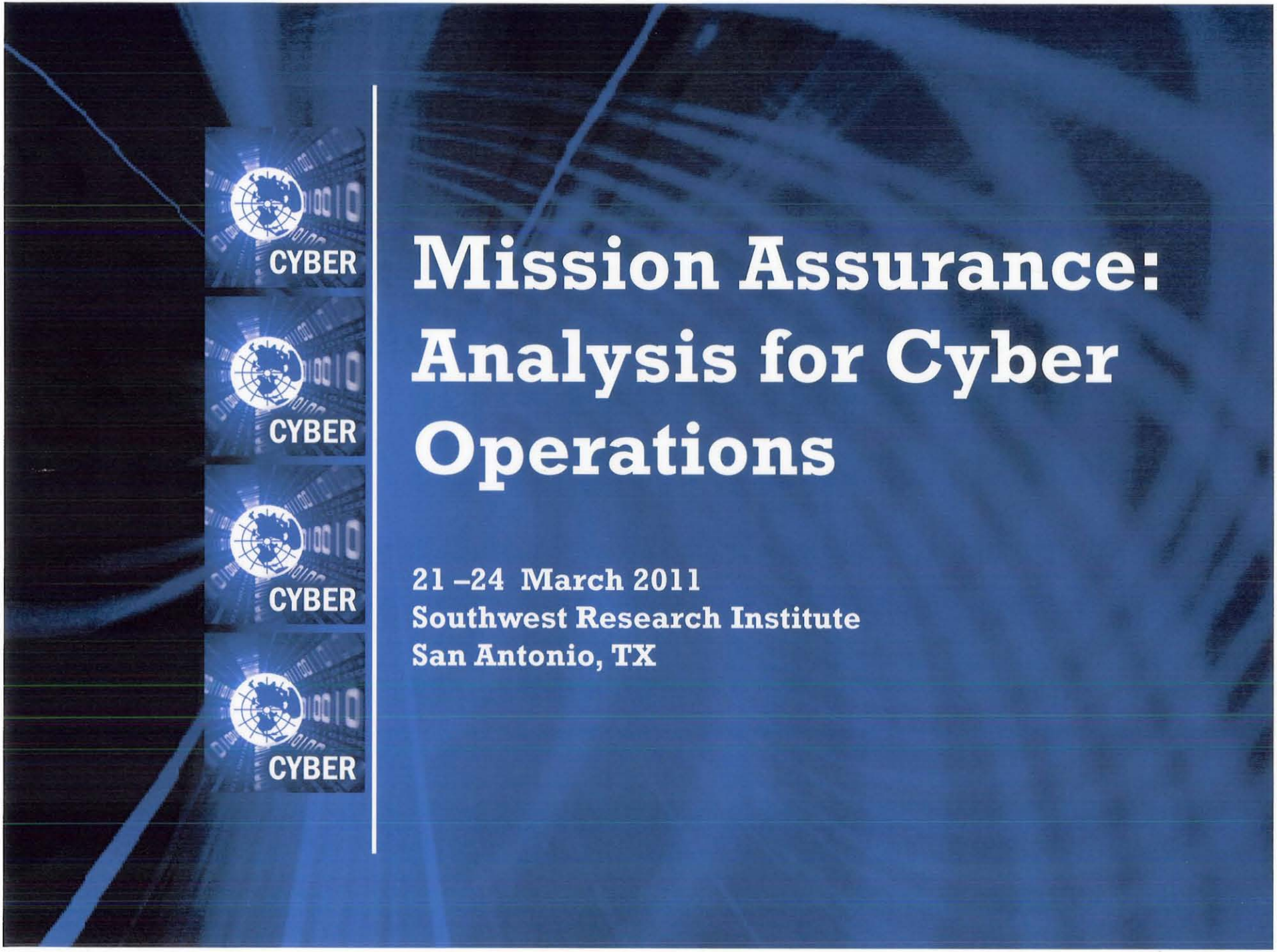

Mission Assurance: Analysis for Cyber Operations

21 –24 March 2011
Southwest Research Institute
San Antonio, TX

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
MAR 2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Situational Awareness	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **USAF HQ A9,Washington,DC,20301**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
MORS Mission Assurance: Analysis for Cyber Operations Special Meeting held in San Antonio, TX Mar 21-24, 2011.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**11**	

Working Group 1 Situational Awareness

Patricia A. Hickman, GS-15
USAF HQ A9

WG Participants

- Patricia Hickman
- Rick Cunningham
- Ed Covert
- Craig Cannon
- Fisher Little
- Akhil Shah
- James Morris
- Mike Shehan
- Brian Bassham
- Ron Farris
- Rex Haddix
- Adam Simonoff
- Sandy Dykes
- Chrysanthie Chamis
- Mark Bishop
- Bruce Moody
- John Sours
- Gene Visco ****

**** = Narc

WG Purpose/Focus

Purpose:

- Define the problems & approaches in greater fidelity based on input from panels
- Develop courses of action or methodologies to reconcile issues identified
- Develop recommendations for DoD leadership on the process / steps needed to develop the structure for and methodology to perform cyber SA assessments

Focus:

- Develop potential characteristics of an initial framework that will enable the scoping and prioritization of cyber SA assessments
- Using the initial framework, develop a proposed scope of DoD cyber and the system attributes for which SA must be assessed
- Using the initial framework, develop a proposed scope for adversary cyber and the system attributes for which SA must be assessed
- Identify potential cyber SA assessment families of tools

Step 1: Top Cyber SA Needs for Mission Assurance

1 – Cyber Environment (INFOCON)

- Abnormal Activity
- Normal Activity

2 – Cyber Health & Status

- Ours
- Partners/Coalition/Commercial

3 – Cyber Capability Impact

- Availability of Forces/Assets
- What is lost if supporting cyber capability goes down?
- What is the impact to an adjacent capability?
- Tradeoff Space? Mitigation Costs?

4 – Mission Impact

- What is the probable degradation to the intended mission?
- What is the likelihood of success?
- Tradeoff Space? Mitigation Costs?

5 - Adversary Cyber Profile

- Who are they? What are they capable of? What are their TTPs?
- What are their vulnerabilities?
- Temporal aspects

6 – Cyber Resiliency

- Reconstitution
- Redundancy
- Mitigation
- Continuity of Operations (COOP)

7 – Cyber Relationships (Authorities)

- Supported
- Supporting
- External (Commercial)

WG1: What we found

- Developing the formal framework that will enable scoping and prioritization of cyber SA assessments is difficult
- Network Management (NM), Computer Network Defense (CND), and Computer Network Attack (CNA) are separate functions that require tailored approaches
  - Clear definitions and delineation are a necessity
  - Responses and reactions vary depending on visibility and mission impact
    - Patti's computer/comms aren't as important as the CC's
  - Urgency, as a function of the mission, needs to be captured
    - Mission assurance and criticality drive system prioritization
- Current Cyber SA is very limited
  - Modeling framework must be flexible so that criteria can be added/subtracted or modified for different scenarios
- Automated data collection and visualization are imperative
  - Allow time to analyze and understand the data to provide insight
  - Reduce latency in decision-making, comprehension, and response
  - Provide a better comprehension of the situation/cyber geography

WG1: Key data questions

Cyber SA Needs
1- Cyber Environment
2- Cyber Health & Status
3- Cyber Capabilities Impact
4- Mission Impact
5- Adversary Cyber Profile
6- Cyber Resiliency
7- Cyber Relationships

- Mission Needs
  - What is the relevance of the data to the mission?
  - Which data has a higher priority?
  - Who should have access to the data?
  - How to filter/compartmentalize sensitive data in a Coalition environment?
- Sources
  - What source provided the data?
  - Can we trust the data source and/or the consolidation of the data?
  - With whom can we share the data?
  - With what frequency is the data provided/refreshed?
  - How can we improve visibility into coalition/partner/service data?
- Attributes
  - Is the data available?
  - How valid is the data?
  - What is the lifespan of the data?
  - Can access to/analysis of the data be automated…Can you trust the algorithm?

WG 1 - Open Questions

- What are the Legal/Policy issues affecting our ability to have the SA we need?
  - Domestic, International, Title Issues
  - National, Departmental, Unit, etc.
- How can we improve Cyber-focused Wargame engagements?
  - Depth of Cyber Order of Battle understanding
- How would we best implement a DIRCYFOR?
- How do we anticipate vulnerabilities associated with emerging technologies?
  - Cloud computing, mobile, social networking, etc.
- Can we define the full spectrum of cyber impacts from the Human Element?
  - Social engineering, shaping/influencing opinions, attack vectors, etc.
- How would we establish a concept/doctrine/process for Cyber Deterrence?
- How do we determine adversary's intent?

WG 1 - Potential Cyber SA Assessment Capabilities

- Comprehensive Cyber Assessment Framework (MOEs & MOPs)
- Cyber Common Operating Picture (COP)
- Cyber Dashboard
  - Supporting Tools
    - Data Collection and Aggregation Tools (Collection point for data from multiple sources; correlation analysis)
    - Visualization Tools, i.e. Malicious Activity or Network Management
  - Techniques
    - Pattern Recognition (Abnormal pattern detection)
      - Neural Networks, Anomaly Detection, Statistical Process Control
    - Epidemiology Modeling (Worm or Malware propagation)
    - Predictive Modeling ("Cyber Weather"??)
    - Agent-based Modeling (Impact of network activity)
    - Game Theory (Risk Analysis)

WG 1 – Way Ahead

- Analyze gaps/shortfalls in cyber support to current missions
- Investigate means for quickly determining lines of authority responses given suspicious activity at known locations (IP addresses)
  - Speeds interagency coordination and decisions on legal implications

WG 1 – Recommendations

- Develop a comprehensive framework that will enable the scoping and prioritization of cyber SA assessments
- Sponsor a study to develop a cyber SA framework
  - Establish a sharable baseline of cyber data to support warfighter analysis
    - Drive POM inputs for cyber capabilities, tools, etc.